UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/551,003	04/03/2006	Azman Bin H J Zahari	05-649	1412

34704 7590 01/17/2008
BACHMAN & LAPOINTE, P.C.
900 CHAPEL STREET
SUITE 1201
NEW HAVEN, CT 06510

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
01/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/551,003	ZAHARI, AZMAN BIN H J	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The Applicant's amendment of 05 November 2007 has been noted and made of record.

2. Claims 1-18 have been presented for examination.

Response to Arguments

3. Applicant's arguments, see page 10, filed 05 November 2007, with respect to the specification have been fully considered and are persuasive. The objection of the specification has been withdrawn.

4. Applicant's arguments with respect to claims 1-18 have been considered but are moot in view of the new grounds of rejection set forth below.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1-5-11 and 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,657,388 to Weiss, hereinafter Weiss, in view of U.S. Patent No. 5,479,512 to Weiss, hereinafter Weiss2.

7. As per claims 1 and 14, Weiss teaches system for secure communication across a communication network comprising:

a personal code generation means having one or more identification codes and one or more encryption codes (Figure 1 [blocks 12, 14, 50], column 2, lines 57-64, i.e. token processor is utilized to generate a one-time, non-predictable code), each identification code and each encryption code being arranged to change with time (column 3, lines 7-11, i.e. time-varying); and

a code server including each identification code and each encryption code (Figure 1 [blocks 16, 60], column 5, lines 4-20), the code server being synchronized with the personal code generation means such that each identification code of the code server change independently of and in synchronization with each identification code of the personal code generation means of the personal code generation means (column 5, line 60 to column 6, line 15);

wherein a user transmits across the communication network (column 5, lines 4-5), each identification code of the personal code generation means and data encrypted with each current encryption code of the personal code generation means and the code server uses each identification code of the code server to authenticate the user and each encryption code of the code server to decrypt the transmitted data (column 2, lines 57-65, column 6, lines 16-28, i.e. inferring the encryption key in order to decrypt data to permit user access to the encrypted data; see figure 2 of U.S.P.N. 5,237,614 as incorporated by reference by Weiss). The Applicant is directed to the discussion of multiple reference 102 rejections at MPEP § 2131.01.

8. Weiss does not teach one or more encryption codes that arranged to vary with time and are synchronized with the server.

9. Weiss2 teaches an encryption key that is a one-time code that is synchronized similarly to that of Weiss (column 6, lines 5-26).

10. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one or more encryption codes that arranged to vary with time and are synchronized with the server, since Weiss2 states at column 6, lines 15-16 that the use of one-time codes as encryption keys enhances security.

11. Regarding claims 2 and 15, Weiss incorporates U.S.P.N. 5,237,614 at column 2 lines 64-65. U.S.P.N. 5,237,614 teaches wherein the code server communicates to the user following authentication of the user by transmitting data across the communication network to the user encrypted with each encryption code of the code server (Figure 2 [block 52], column 9, lines 15-35) and the user decrypts the data transmitted by the code server with each encryption code of the personal code generation means (Figure 2 [block 56], column 9, lines 36-51).

12. Regarding claim 3, 4, and 16, Weiss teaches wherein the code server stores information including a username and password assigned to the owner of the personal code generation means and the password is transmitted across the communication network and the code server uses the password to authenticate the user as the owner (column 1, lines 42-57).

13. Weiss and Weiss2 do not teach that the username and password is transmitted with each identification code of the personal code generation means and the data encrypted with each encryption code and the code server uses the password to authenticate the user as the owner of the personal code generation means of the personal code generation means.

14. It would have been obvious to one of ordinary skill in the art at the time the invention was made to transmit the username and password with the identification code and encryption code and using the password to authenticate the user, since Weiss teaches at column 2, lines 11-18 that varying the token information improves the security, as well as provides at least two forms of authentication of the user thereby providing better security.

15. Regarding claim 5, Weiss teaches wherein the personal code generation means comprises a personal portable token (Figure 1 [blocks 12, 14], column 4, lines 27-49).

16. With regards to claim 6, the Examiner interprets a pendant as any hanging ornament, as an earring or the main piece suspended from a necklace. The definition courtesy of *Dictionary.com Unabridged (v 1.1)*. Random House, Inc. 23 Apr. 2007. <Dictionary.com http://dictionary.reference.com/browse/pendant>. The Examiner contends that it is well known in the art that the personal portable token is a pendant and the Applicant now admits as such.

17. With regards to claim 7, Weiss teaches wherein the personal portable token is a card (column 2, lines 18-34).

18. With regards to claim 8, Weiss teaches wherein the personal code generation means includes a communication port to communicate each identification code of the personal code generation means and each current encryption code of the personal code generation means to a user's computer (column 5, lines 21-37).

19. Regarding claim 9, Weiss teaches wherein the personal code generation means comprises software residing on a user's computer (column 2, lines 46-56, column 4, lines 44-58, i.e. machine readable form).

20. With regards to claim 10, Weiss teaches wherein the personal code generation means includes a display means (column 4, lines 46-49, i.e. laptops, notebook computers, and PDA devices all have display means). The Applicant admits that it is well known in the art that the display means displaying each identification code of the personal code generation means and each encryption code of the personal code generation means.

21. With regards to claim 11, Weiss teaches wherein the personal code generation means comprises a smart card having an initialization code known to the code server and software residing on a user's computer (column 2, lines 18-34), the software being capable of generating each identification code and each encryption code based on the initialization code and a reference clock (column 7, lines 49-60), the code server also being capable of generating each identification code and each encryption code based on the initialization code and the reference clock (column 5, line 60 to column 6, line 15).

22. Claims 12, 13, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss in view of Weiss2, and in further view of U.S. Patent No. 6,981,141 to Mahne et al., hereinafter Mahne.

23. As per claims 12 and 17, Weiss teaches a system for securely accessing data stored in an encrypted form on a storage means accessible by a communication network comprising:

a personal code generation means having one or more identification codes (Figure 1 [blocks 12, 14, 50], column 2, lines 57-64, i.e. token processor is utilized to generate a one-time,

non-predictable code), each identification code being arranged to change with time (column 3, lines 7-11, i.e. time-varying);

a code server including each identification code and each encryption code (Figure 1 [blocks 16, 60], column 5, lines 4-20), the code server being synchronized with the personal code generation means such that each identification code of the code server of the server change independently of and in synchronization with each identification code of the personal code generation means of the personal code generation means, the code server also having a previous archiving code being the archiving code last used to encrypt the key archive and a current archiving code being arranged to change with time (column 5, line 60 to column 6, line 15);

wherein when a user wishes to access each stored data file, the user transmits across the communication network (column 5, lines 4-5), each identification code of the personal code generation means and data including a request to access the stored data files encrypted with each encryption code of the personal code generation means and the code server uses each identification code of the code server to authenticate the user and each encryption code of the code server to decrypt the transmitted data and the code server communicates to the user the previous archiving code in encrypted form using each encryption code of the code server so that the user may decrypt the data to provide access to the stored data files (column 2, lines 57-65, column 6, lines 16-28, i.e. inferring the encryption key in order to decrypt data to permit user access to the encrypted data; see figure 2 of U.S.P.N. 5,237,614 as incorporated by reference by Weiss).

24. Weiss does not teach one or more encryption codes that arranged to vary with time and are synchronized with the server, a key archive associated with the personal code generation

means and with one or more data files on the storage means, the key archive having information including the location of the data files and the encryption codes with which each of the data files is encrypted, the key archive being encrypted with an archiving code; and decrypting the key archive providing access to the stored data files.

25. Weiss2 teaches an encryption key that is a one-time code that is synchronized similarly to that of Weiss (column 6, lines 5-26).

26. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use one or more encryption codes that arranged to vary with time and are synchronized with the server, since Weiss2 states at column 6, lines 15-16 that the use of one-time codes as encryption keys enhances security.

27. Mahne discloses a key table stored on a smart card which stores encryption keys used to decrypt files (column 8, lines 56-67, column 9, lines 43-50).

28. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a key archive associated with the personal code generation means and with one or more data files on the storage means, the key archive having information including the location of the data files and the encryption codes with which each of the data files is encrypted, the key archive being encrypted with an archiving code; and decrypting the key archive providing access to the stored data files, since Mahne states at column 3, line 65 to column 4, line 2 that incorporating the key archive would provide an easy to use and inexpensive technology that would allow users to conveniently access encrypted documents and files.

29. Regarding claims 13 and 18, Mahne teaches wherein when the code server transmits to the user the previous archiving code, the code server also transmits the current archiving code and the user then uses the current archiving code to encrypt the key archive when the user has completed accessing the stored data files and the code server stores the current archiving code as the previous archiving code for future access to the store data files (column 8, lines 56-67, column 9, lines 43-50).

Conclusion

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

31. The following patents are cited to further show the state of the art with respect to one-time codes, such as:

United States Patent Application Publication No. 2004/0236819 A1 to Anati et al., which is cited to show encryption using a one time code, for example, see paragraph 0055.

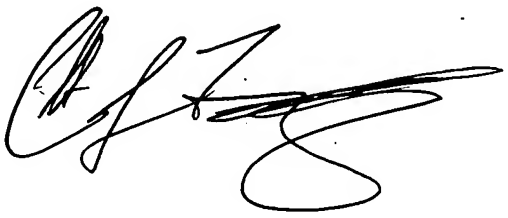
United States Patent No. 5,988,497 to Wallace, which is cited to show authentication using smart cards that generate variable PIN numbers.

32. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

33. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

34. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Christian LaForgia
P0061tent Examiner
Art Unit 2131



clf